

Description :

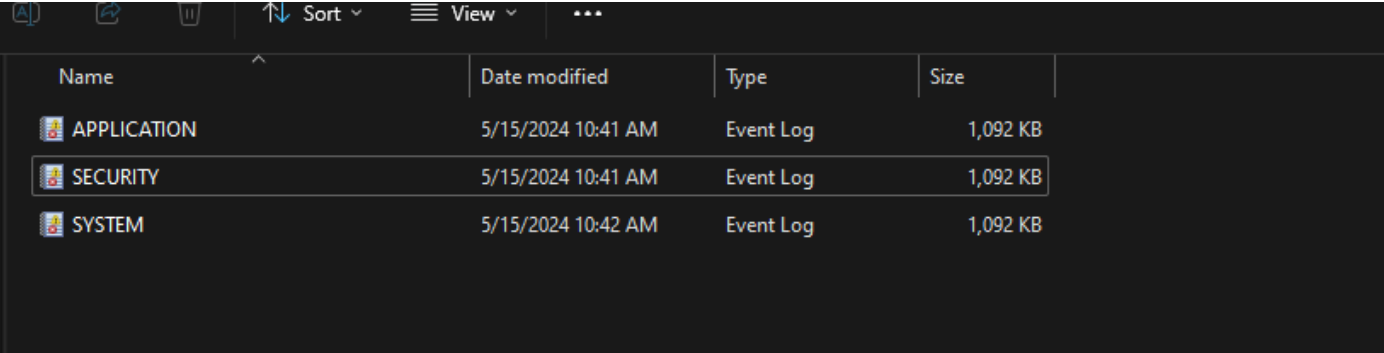
In this very easy sherlock, you will learn how to detect NTDS.dit dumping which is one of the most critical Active directory attacks. You will get your hands on event logs to respond to an attack where the attacker utilized ntdsutil utility to dump the NTDS.dit database.

Scenario :

Forela's Domain environment is pure chaos. Just got another alert from the Domain controller of NTDS.dit database being exfiltrated. Just one day prior you responded to an alert on the same domain controller where an attacker dumped NTDS.dit via vssadmin utility. However, you managed to delete the dumped files kick the attacker out of the DC, and restore a clean snapshot. Now they again managed to access DC with a domain admin account with their persistent access in the environment. This time they are abusing ntdsutil to dump the database. Help Forela in these chaotic times!!

Initial Analysis :

We start off by viewing the artifacts provided to us.



Name	Date modified	Type	Size
APPLICATION	5/15/2024 10:41 AM	Event Log	1,092 KB
SECURITY	5/15/2024 10:41 AM	Event Log	1,092 KB
SYSTEM	5/15/2024 10:42 AM	Event Log	1,092 KB

Event Logs

An event log is a file that contains information about usage and operations of operating systems, applications or devices. Security professionals or automated security systems like SIEMs can access this data to manage security, performance, and troubleshoot IT issues.

Security event log contain events related to security, such as login attempts, object access, and file deletion. Administrators determine which events to log, in accordance with their audit policy.

Application logs contain events logged by applications. Which events get logged is determined by the application developers.

System logs contain events logged by the operating system, such as driver issues during startup.

Analysis :

Q1 When utilizing ntdsutil.exe to dump NTDS on disk, it simultaneously employs the Microsoft Shadow Copy Service. What is the most recent timestamp at which this service entered the running state, signifying the possible initiation of the NTDS dumping process?

Hint : In the System event log, filter for Event ID 7036 and look for the mentioned service name. Once spotted, go to the details tab, and expand the System option to get the event time in UTC.

Lets start by opening the system event log and filter for Event ID 7036.

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

Task category:

Keywords:

User:

<All Users>

Computer(s):

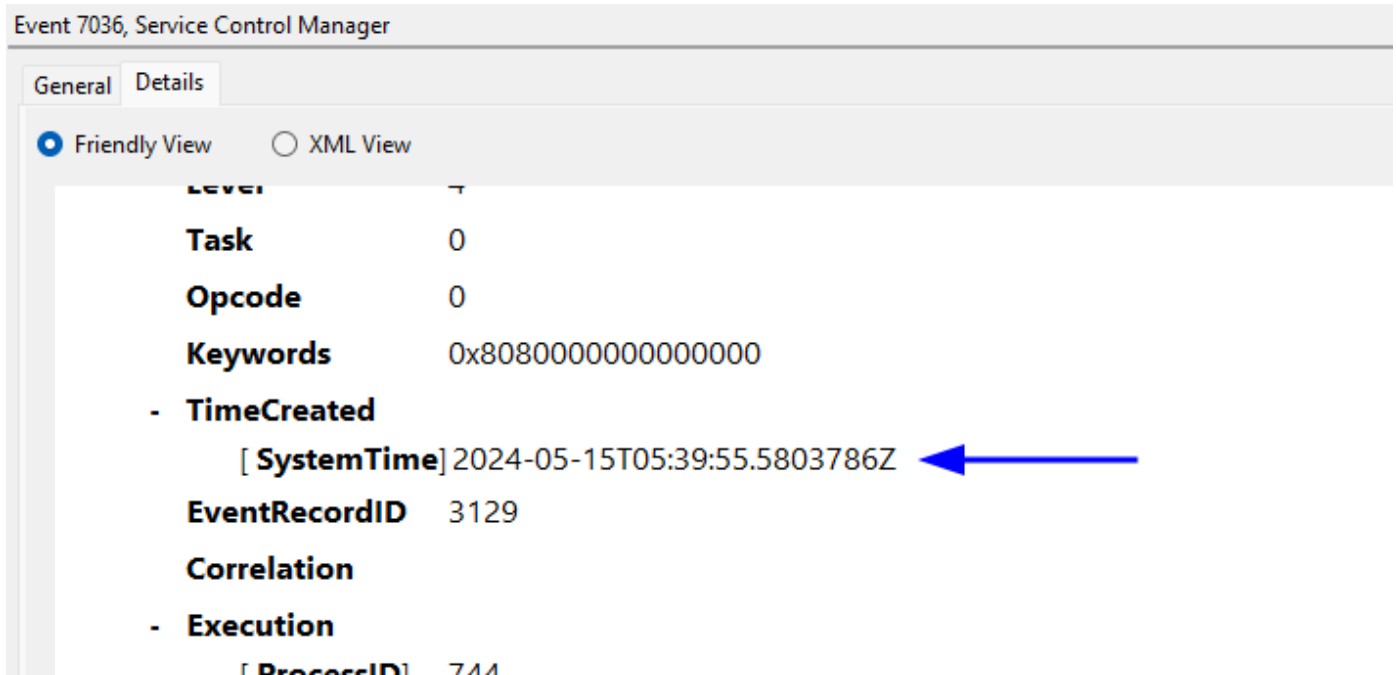
<All Computers>

Clear

Searching for Microsoft Shadow Copy Service, we stumble upon the event when this service started running.

Information	5/15/2024 10:40:18 AM	Service Control Manager
Information	5/15/2024 10:39:55 AM	Service Control Manager
Event 7036, Service Control Manager		
General Details		
The Volume Shadow Copy service entered the running state.		

Lets see its UTC time by going in details tab.

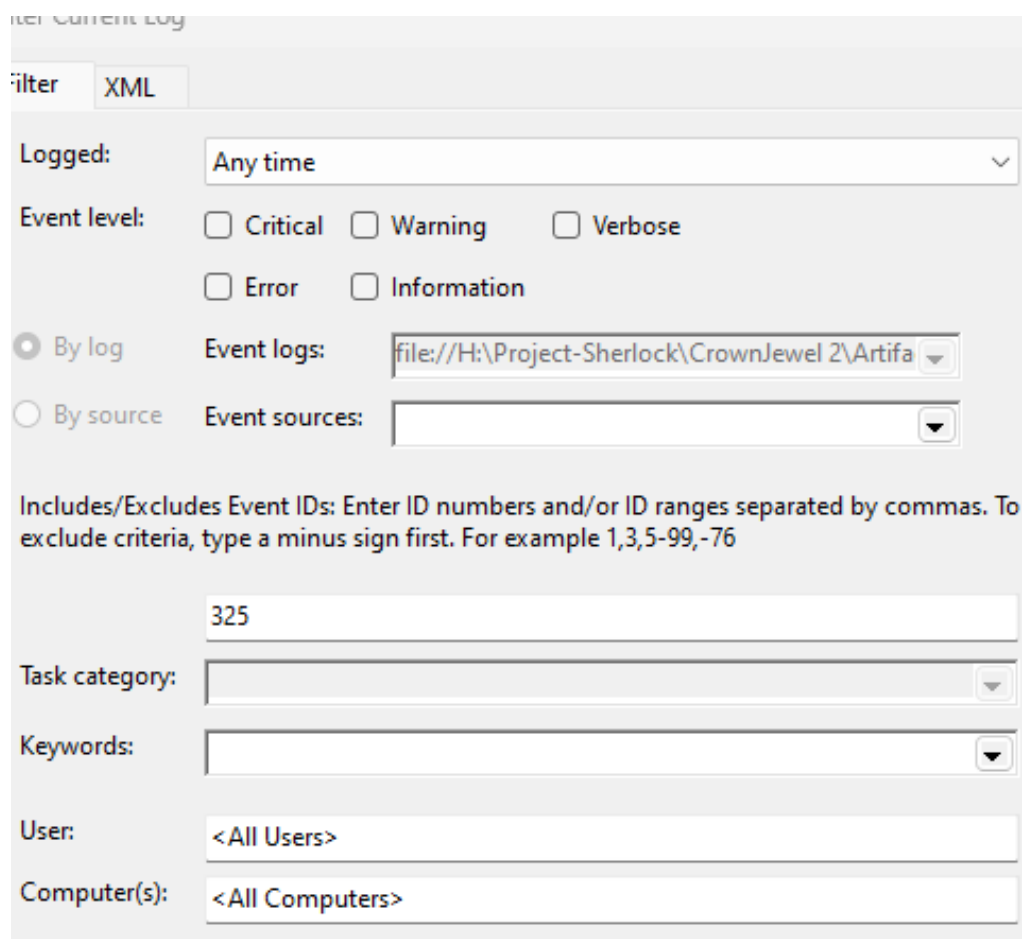


Answer: 2024-05-15 05:39:55

Q2 Identify the full path of the dumped NTDS file.

Hint : In Application Event Log, filter for Event ID 325. This Event ID is recorded whenever a new database (new copy of NTDS.dit database) is created by the database engine.

Open the application log file and filter for Event ID 325.



Look for the event around the established timeline from previous question. We only spot 1 event on supposed day of attack.

Event 325, ESENT

GeneralDetails

NTDS (3940,D,100) The database engine created a new database (2, C:\Windows\Temp\dump_tmp\Active Directory\ntds.dit). (Time=0 seconds)

Additional Data:
dbv = 1568.20.0 (36)

Internal Timing Sequence:
[1] 0.000402 +J(0) +M(C:0K, Fs:17, WS:68K # 68K, PF:20K # 20K, P:20K)
[2] 0.000002 +J(0) +M(C:0K, Fs:1, WS:4K # 4K, PF:0K # 0K, P:0K)
[3] 0.004469 +J(0) +M(C:16K, Fs:14, WS:48K # 56K, PF:36K # 44K, P:36K)
[4] 0.000100 +J(0)
[5] 0.000057 +J(CM:0, PgRf:3, Rd:0/0, Dy:3/3, Lg:0/0) +M(C:-16K, Fs:16, WS:48K # 40K, PF:-16K # 0K, P:-16K)
[6] 0.059418 -0.000591 (3) CM -0.058075 (6) WT +J(CM:3, PgRf:213, Rd:0/3, Dy:20/200, Lg:0/0) +M(C:80K, Fs:74, WS:240K # 240K, PF:280K # 260K, P:280K)
[7] 0.000316 +J(0) +M(C:0K, Fs:2, WS:8K # 8K, PF:0K # 0K, P:0K)
[8] 0.000001 +J(0)
[9] 0.000718 -0.000360 (3) WT +J(0) +M(C:-28K, Fs:10, WS:-20K # 8K, PF:-28K # 8K, P:-28K)
[10] 0.015953 -0.000330 (3) CM -0.014071 (6) WT +J(CM:3, PgRf:354, Rd:0/3, Dy:14/41, Lg:0/0) +M(C:44K, Fs:44, WS:136K # 116K, PF:112K # 80K, P:112K)
[11] 0.000001 +J(0).

Answer: C:\Windows\Temp\dump_tmp\Active Directory\ntds.dit

Q3 When was the database dump created on the disk?

Hint : This would be the time of the same event when database copy was created(Event ID 325).

Go to details tab for the event identified in previous question.

Event 325, ESENT

GeneralDetails

☒ Friendly View ☐ XML View

Task1

Opcode0

Keywords0x8000000000000000

- TimeCreated

[SystemTime] 2024-05-15T05:39:56.5025731Z

EventRecordID646

Correlation

- Execution

[ProcessID] 0

[ThreadID] 0

Answer: 2024-05-15 05:39:56

Q4 When was the newly dumped database considered complete and ready for use?

Hint: In Application Event Log, filter for Event ID 327. This Event ID is recorded whenever a newly created database (new copy of NTDS.dit database) is detached by the database engine and marked ready to use.

In same log filer now add new filter for Event ID 327. We only get 2 events

APPLICATION_2 Number of events: 653		
Filtered: Log: file://H:\Project-Sherlock\CrownJewel 2\Artifacts\APPLICATION.evtx; Source: ; Event ID: 327. Number of events: 2		
Level	Date and Time	Source
Information	5/15/2024 10:39:58 AM	ESENT
Information	5/15/2024 10:39:58 AM	ESENT

Both events are related to the attack as we can see from the timestamps.

Note : Its important to note that the timestamp in events viewer pane is showed in Timestamp configured for PC which in my case is UTC+5. The UTC Time can be seen from Details tab.

Event 327, ESENT	
General	Details
<input checked="" type="radio"/> Friendly View <input type="radio"/> XML View	
Version	0
Level	4
Task	1
Opcode	0
Keywords	0x8000000000000000
- TimeCreated	[SystemTime] 2024-05-15T05:39:58.5647753Z
EventRecordID	649
Correlation	
- Execution	[ProcessID] 0

Answer: 2024-05-15 05:39:58

Q5 Event logs use event sources to track events coming from different sources. Which event source provides database status data like creation and detachment?
Hint : Look at the Event source in Events from question 2 to 4.

Looking at source from application events we have been analyzing so far we can see it is ESENT.

ifacts\APPLICATION.evtx; Source: ; Event ID: 327. Number of events: 2	
Date and Time	Source
5/15/2024 10:39:58 AM	ESENT
5/15/2024 10:39:58 AM	ESENT

Answer: ESENT

Q6 When ntdsutil.exe is used to dump the database, it enumerates certain user groups to validate the privileges of the account being used. Which two groups are enumerated by the ntdsutil.exe process? Also, find the Logon ID so we can easily track the malicious session in our hunt.

Hint : In Security Logs, filter for Event ID 4799 . Look for Events in between the timeframe of incident identified so far. Identify the events where process name is C:\Windows\System32\ntdsutil.exe .

Now we open Security log and filter for Event ID 4799. Keeping the timeline in mind, we need to find events related to ntdsutil process. We find many events of such criteria all occurring in total of 2 seconds , also falls under the timeframe of our incident.

Security Log Details	
A security-enabled local group membership was enumerated.	
Subject:	
Security ID:	S-1-5-21-3239415629-1862073780-2394361899-500
Account Name:	Administrator
Account Domain:	FORELA
Logon ID:	0x8DE3D
Group:	
Security ID:	BUILTIN\Administrators
Group Name:	Administrators
Group Domain:	Builtin
Process Information:	
Process ID:	0xf64
Process Name:	C:\Windows\System32\ntdsutil.exe



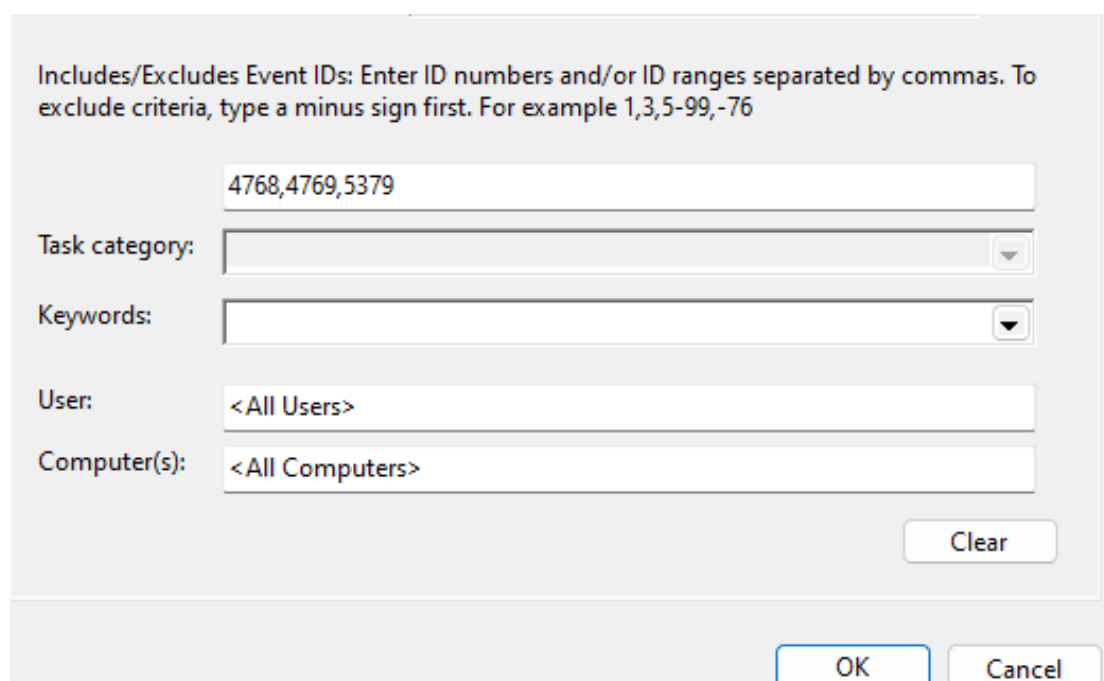
We can see the User groups being targeted and the Logon ID as well.

Answer: Administrators, Backup Operators, 0x8DE3D

Q7 Now you are tasked to find the Login Time for the malicious Session. Using the Logon ID, find the Time when the user logon session started.

Hint : Since this is a domain environment we would want to use Kerberos events to find the timestamp. Filter for Event ID 4768 and 4769. From here identify the Event Where Account Name is a user account name and not any service or machine account (Starting with a \$) in the event 4768. This event will be immediately followed by a 4769 event with the same Subject Username. Now add another event id 5379 in the filter. These new events have the Logon ID we are tracking. Notice that timestamp of all these events are same as they happened right after each other. This will be the logon time

Logon IDs are used to track Logons on windows systems. We filter for Event ID 4768,4769 and 5379 , and look for events with a user account name and not a service/machine account.



Level	Date and Time	Event ID	Task Category	Source
Information	5/15/2024 10:36:35 AM	5379	User Account Management	Microsoft Windows security auditing.
Information	5/15/2024 10:36:31 AM	5379	User Account Management	Microsoft Windows security auditing.
Information	5/15/2024 10:36:31 AM	5379	User Account Management	Microsoft Windows security auditing.
Information	5/15/2024 10:36:31 AM	5379	User Account Management	Microsoft Windows security auditing.
Information	5/15/2024 10:36:31 AM	4769	Kerberos Service Ticket Operations	Microsoft Windows security auditing.
Information	5/15/2024 10:36:31 AM	4768	Kerberos Authentication Service	Microsoft Windows security auditing.
Information	5/15/2024 10:36:18 AM	4769	Kerberos Service Ticket Operations	Microsoft Windows security auditing.

Event 4768, Microsoft Windows security auditing.

General Details

A Kerberos authentication ticket (TGT) was requested.

Account Information:

Account Name: Administrator
 Supplied Realm Name: FORELA
 User ID: S-1-5-21-3239415629-1862073780-2394361899-500

Service Information:

Service Name: krbtgt
 Service ID: S-1-5-21-3239415629-1862073780-2394361899-502

Network Information:

Client Address: ::1
 Client Port: 0

Additional Information:

Ticket Options: 0x40810010
 Result Code: 0x0

We can see Event ID 5379 right after kerberos events. Lets open a event to see the Logon ID.

General Details

Credential Manager credentials were read.

Subject:

Security ID: S-1-5-21-3239415629-1862073780-2394361899-500
 Account Name: Administrator
 Account Domain: FORELA
 Logon ID: 0x8DE3D
 Read Operation: Enumerate Credentials

This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Answer: 2024-05-15 05:36:31